ACTA ARITHMETICA
Online First version

Irreducible Sobol' sequences in prime power bases

by

Henri Faure (Marseille) and Christiane Lemieux (Waterloo)

1. Introduction. The family of low-discrepancy sequences introduced by Sobol' in his 1967 paper [19] has had a tremendous impact on the field of quasi-Monte Carlo methods. Two important ways in which this impact has taken place are: 1) it gave rise to several other important contributions giving variations, extensions, and generalizations of this construction and the concepts used to study it; 2) despite all the generalizations that have been proposed, this construction continues to play an important role in the application of quasi-Monte Carlo methods in practice, with implementations offered in many software/calculation packages [1, 9, 10, 11, 23, 24].

The goal of this work is to study generalizations of Sobol' sequences that preserve two fundamental properties of the original construction, namely: (a) one-dimensional projections that are $(0, 1)$-sequences, and (b) an easy-to-implement column-by-column construction for the generating matrices, based on linear recurrences determined by monic irreducible polynomials over $\mathbb{F}_b$, where b is a prime power. We compare this generalization—which, as announced in the title, we call "irreducible Sobol' sequences in prime power bases"—with other closely related families of digital (t, s)-sequences. In particular, we describe in detail how our construction is included in the larger family of generalized Niederreiter sequences introduced by Tezuka [20].

The paper is organized as follows. In Section 2, we recall different frameworks to build the low-discrepancy sequences that are relevant to this work. Section 3 is devoted to connections between Niederreiter sequences in base 2 and Sobol' sequences, with our generalization of the latter introduced in Section 4, along with a description of its relation to generalized Niederreiter

2010 *Mathematics Subject Classification*: Primary 11K38; Secondary 11K06.
Key words and phrases: low-discrepancy sequences, Sobol' sequences, Niederreiter sequences, generalized Niederreiter sequences.
Received 13 July 2015; revised 11 January 2016.
Published online *.

DOI: 10.4064/aa8226-1-2016

sequences. An analysis similar to the one in Section 3 for the base 2 case is performed in Section 5 for the generalized constructions in prime power bases. We conclude with some final remarks in Section 6.

The remainder of this section is devoted to recalling the basic concepts that will be used throughout this paper, starting with the notion of discrepancy, which measures the uniformity properties of sequences of points in the unit hypercube $I^s := [0,1)^s$.

Consider a point set $P_N = \{X_1, \ldots, X_N\} \subseteq I^s$, and denote by $\mathcal{J}^*$ the set of intervals J of I^s of the form $J = \prod_{j=1}^{s}[0, z_j)$. Then the *discrepancy function* of P_N on J is the difference

$$E(J; N) = A(J; P_N) - NV(J),$$

where $A(J; P_N) = \#\{n : 1 \leq n \leq N,\ X_n \in J\}$ is the number of points in P_N that fall in the subinterval J, and $V(J) = \prod_{j=1}^{s} z_j$ is the volume of J.

Then, the *star* (*extreme*) *discrepancy* D^* of P_N is defined as

$$D_N^* = \sup_{J \in \mathcal{J}^*} |E(J; N)|.$$

A sequence of points $(X_n)_{n\geq 1}$ in I^s is said to be a *low-discrepancy sequence* if the (star) discrepancy D_N^* of its first N points satisfies $D_N^* \in O((\log N)^s)$.

The constructions in this paper achieve this low-discrepancy property by focusing on b-adic intervals of $[0,1)^s$ in the definition of D_N^* above. That is, they are built so that an appropriate number of points is placed in intervals of the form

$$E = \prod_{i=1}^{s} [a_i b^{-q_i}, (a_i + 1)b^{-q_i})$$

(called *elementary intervals*) with integers $q_i \geq 0$ and $0 \leq a_i < b^{q_i}$ for $1 \leq i \leq s$. Hence E is of volume b^{-q}, where $q = \sum_{i=1}^{s} q_i$. A point set $P_N \subseteq I^s$ with $N = b^m$ points is said to be a (t, m, s)-*net* if every interval E with $q = \sum_{i=1}^{s} q_i \leq m - t$ contains b^{m-q} points. It should be clear that a smaller value of t yields better uniformity properties for P_N.

To introduce the concept of (t, s)-sequence, we first need to define the truncation operator introduced by Tezuka [20] and then Niederreiter and Xing [16, 17] to handle new constructions for low-discrepancy sequences.

Let $X = \sum_{l=1}^{\infty} h_l b^{-l}$ be a b-adic expansion of $X \in [0,1]$, with the possibility that $h_l = b - 1$ for all but finitely many l. For every integer $m \geq 1$, the m-*truncation* of X is given by $[X]_{b,m} = \sum_{l=1}^{m} h_l b^{-l}$ (depending on X via its expansion). In the case where $X \in I^s$, the notation $[X]_{b,m}$ means the m-truncation is applied to each coordinate of X.

An s-dimensional sequence $(X_n)_{n\geq 1}$, with prescribed b-adic expansions for all coordinates, is a (t, s)-*sequence* (*in the broad sense*) if the point set

$\{[X_n]_{b,m} : kb^m < n \le (k+1)b^m\}$ is a (t, m, s)-net in base b for all integers $k \ge 0$ and $m \ge t$.

Niederreiter [14] proved that the equidistribution property of (t, s)-sequences over intervals of the form E was sufficient to ensure these sequences had a low discrepancy, as stated in the next result. Note that this property was established in [19] and [4] for the specific constructions introduced in these earlier papers. It reads as follows:

The first $N \ge 1$ points of a (t, s)-sequence in base b satisfy

$$D_N^* \le c_s(\log N)^s + O((\log N)^{s-1}), \tag{1.1}$$

where c_s is a constant depending only on s.

The low-discrepancy sequences of interest in this paper are (t, s)-sequences that all fit within the *digital method* introduced by Niederreiter [14], which we now describe. Let $b \ge 2$. We first need to choose:

(1) a commutative ring R with identity and $\mathrm{card}(R) = b$;
(2) bijections $\psi_r : \mathbb{Z}_b \to R$;
(3) bijections $\lambda_{i,j} : R \to \mathbb{Z}_b$ for $j \ge 1$ and $1 \le i \le s$;
(4) $\infty \times \infty$ generating matrices $C^{(1)}, \ldots, C^{(s)}$ over R with elements denoted as $c_{j,r}^{(i)}$, and rows denoted by $\boldsymbol{c}_j^{(i)}$, for $j, r \ge 1$.

Note that for b a prime power, the ring R is taken to be the finite field $\mathbb{F}_b$ of order b.

Now, for $n \ge 1$, let

$$n - 1 = \sum_{r=0}^{\infty} a_r(n) b^r$$

be the expansion of $n - 1$ in base b, where $a_r(n) \in \mathbb{Z}_b$ and $a_r(n) = 0$ for r sufficiently large. Let $\boldsymbol{n}$ be the vector in R^∞ whose rth component is given by $n_r = \psi_r(a_{r-1}(n))$, $r \ge 1$. Then let

$$X_{n,j}^{(i)} = \lambda_{i,j}(\boldsymbol{c}_j^{(i)} \cdot \boldsymbol{n}) = \lambda_{i,j}\Big(\sum_{r=1}^{\infty} c_{j,r}^{(i)} n_r\Big),$$

and define $X_n^{(i)} = \sum_{j=1}^{\infty} X_{n,j}^{(i)} b^{-j}$. The sequence of points obtained by this digital method is given by $(X_n)_{n \ge 1}$ with $X_n = (X_n^{(1)}, \ldots, X_n^{(s)})$.

A desirable property for a (t, s)-sequence is to have one-dimensional projections that are all $(0, 1)$-sequences. In turn, this requires that the first $m \times m$ entries of each generating matrix form a non-singular matrix for all $m \ge 1$, a condition that is satisfied when using non-singular upper triangular (NUT) matrices. The Sobol' and $(0, s)$-sequences introduced respectively in [19] and [4] are both based on NUT generating matrices. But this is not

necessarily the case for the generalizations that will be discussed in the next section, namely for Niederreiter [15] and generalized Niederreiter [20] sequences. As mentioned previously, one way in which our proposed generalization of Sobol' sequences differs from these other ones is that it preserves this useful property of having NUT generating matrices.

2. Frameworks for the construction of (t, s)-sequences

2.1. The framework of Sobol'. The construction introduced by Sobol' [19], mentioned in the introduction, was originally named LP_τ-sequences, but is now widely known as *Sobol' sequences*. It was the first digital sequence that was proposed. It is defined in base 2, which makes its sequence generation very fast, a property that has contributed to its popularity with practitioners. For this sequence, the generating matrices $C^{(i)}$ in the digital method are constructed column by column, using monocyclic operators (obtained from primitive polynomials over $\mathbb{F}_2$) and so-called *direction numbers*, which are used to initialize the first columns of the generating matrices.

To simplify the presentation, we explain how to construct a given generating matrix based on a primitive polynomial $p(x)$ over $\mathbb{F}_2[x]$, thus dropping for now the index i denoting the dimension $1 \le i \le s$ considered.

Let $p(x) = a_e x^e + a_{e-1}x^{e-1} + \cdots + a_1 x + a_0$ be a primitive polynomial in $\mathbb{F}_2[x]$ of degree $e \ge 1$. Let V_r be a column vector of infinite length with entries in $\mathbb{F}_2$, with its jth entry denoted $v_{j,r}$, for $j, r \ge 1$. For $r = 1, \ldots, e$, let d_r be an odd number between 1 and 2^r, and let the first e entries of $V_1, \ldots, V_r$ be defined via

$$\frac{d_r}{2^r} = \sum_{j=1}^{r} v_{j,r} 2^{-j}$$

and $v_{j,r} = 0$ for $j > r$. Note that since d_r is odd, $v_{r,r} = 1$ for $r = 1, \ldots, e$. The e integers $d_1, \ldots, d_e$ are called the *direction numbers* associated with $p(x)$. The remaining vectors V_j for $j > e$ are obtained using the following linear recurrence associated with $p(x)$:

$$V_{r+e} = \frac{1}{2^e} a_0 V_r + a_0 V_r + a_1 V_{r+1} + \cdots + a_{e-1} V_{r+e-1}, \quad r \ge 1, \tag{2.1}$$

where $1/2^e$ in the first term indicates that we multiply by 2^{-e} the fraction whose binary expansion is contained in V_r, or equivalently, the jth entry of $(1/2^e)V_r$ is given by the $(j-e)$th entry of V_r for $j > e$, while the first e entries are 0.

The generating matrix C is then obtained by taking V_r as its rth column, for $r \ge 1$. It is easy to see from (2.1) and the property that $v_{r,r} = 1$ for $r = 1, \ldots, e$ (by definition of the direction numbers) that the matrix C is NUT and therefore yields a $(0, 1)$-sequence.

We point out that Sobol' uses the term *direction numbers* for all vectors V_r, $r \geq 1$, while we call *direction numbers* only the first e ones giving the first e columns of C. Hence, in terms of generating matrices, the direction numbers associated with $p(x)$ can be defined as the NUT $e \times e$ *direction matrix* $D = (v_{j,r})_{1 \leq j \leq r \leq e}$ (the first infinite vectors V_r of C being filled in with zeros).

As shown in [19] (but using a different terminology), Sobol' sequences are (t, s)-sequences in base 2 with $t = \sum_{i=1}^{s}(e_i - 1)$, where e_i is the degree of the primitive polynomial used to construct the ith generating matrix.

2.2. The framework of Faure–Niederreiter. The second family of digital (t, s)-sequences that was proposed by the first author [4] was the construction for $(0, s)$-sequences in a prime base $b \geq s$, later generalized to prime power bases $b \geq s$ by Niederreiter [14]. The key idea to get the optimal value of 0 for t is to work with the NUT Pascal matrix P over $\mathbb{F}_b$, whose element in the jth row and rth column is given by

$$P_{j,r} = \binom{r-1}{j-1}$$

for $r \geq j \geq 1$. The ith generating matrix is then obtained as $C^{(i)} = P^{i-1}$ for $i = 1, \ldots, s$. As noted in [4, Sect. 3.1], this implies that for $2 \leq i \leq s$, $C^{(i)}$ has entries of the form

$$c_{j,r}^{(i)} = (i-1)^{r-j}\binom{r-1}{j-1} \tag{2.2}$$

for $r \geq j \geq 1$.

The construction proposed in [14, Thm. 6.18] extends the above *Faure sequences* to prime power bases b. The matrices $C^{(i)}$ are defined similarly to the above, but with the term $i - 1$ in (2.2) replaced by some element β_i of $\mathbb{F}_b$, with β_i's distinct for $i = 2, \ldots, s$. Note that the construction in [14, Thm. 6.18] is in fact defined for arbitrary bases b, but as discussed in [14, Cors. 6.19 and 6.20], the restriction to prime power bases ensures the existence of a $(0, s)$-sequence for any $s \leq b$, while for arbitrary bases this can only be ensured if $s \leq 2$. Hence the appropriate generalization of Faure sequences from [4] is the one based on prime power bases.

2.3. The framework of Niederreiter. The next family of constructions are the *Niederreiter sequences* introduced by Niederreiter [15]. Although this construction is described for a general base b in [15, Sect. 4], here we assume b is a prime power. The construction requires s pairwise coprime polynomials $p_1(x), \ldots, p_s(x) \in \mathbb{F}_b[x]$ of respective positive degrees e_i, and then a series of polynomials $g_{i,j}(x) \in \mathbb{F}_b[x]$ for $i = 1, \ldots, s$ and $j \geq 1$ such that $\gcd(p_i(x), g_{i,j}(x)) = 1$ for all i, j. The generating matrices are defined through their rows by first developing the formal Laurent series (where

$0 \le k < e_i$, and $w \le 1$ may depend on i, j, k)

$$\frac{x^k g_{i,j}(x)}{p_i(x)^j} = \sum_{r=w}^{\infty} a^{(i)}(j,k,r) x^{-r}. \tag{2.3}$$

The elements of the generating matrices are then defined as

$$c_{j,r}^{(i)} = a^{(i)}(q+1, u, r)$$

for $r \ge 1$, and where q and u depend on i and j through the relation $j - 1 = qe_i + u$ with $0 \le u \le e_i - 1$.

Let us explain in more detail the "mechanics" behind this definition for a given i. Consider the first block of e_i rows of $C^{(i)}$. The $(k+1)$th row is obtained via the coefficients $a^{(i)}(1,k,r)$ of the formal Laurent series of $x^k g_{i,1}(x)/p_i(x)$. To get the next block of e_i rows, we change the polynomial $g_{i,1}(x)$ to $g_{i,2}(x)$ and raise the power $p_i(x)$ used in the denominator to 2, i.e., the $(e_i + k + 1)$th row contains the coefficients of the formal Laurent series of $x^k g_{i,2}(x)/(p_i(x))^2$, for $k = 0, \ldots, e_i - 1$. The jth block of e_i rows is obtained in a similar fashion, using the polynomial $g_{i,j}(x)$ in the numerator and raising $p_i(x)$ to the power j in the denominator.

It is shown in [15] that the construction thus obtained is a digital (t,s)-sequence in base b with $t = \sum_{i=1}^{s}(e_i - 1)$, provided $\lim_{j\to\infty}(je_i - \deg(g_{i,j})) = \infty$ for all $1 \le i \le s$. This formula for t is also valid for the Sobol' sequence, as explained in Section 2.1, but with primitive polynomials. Here, however, the requirement on the polynomials $p_i(x)$ is that they be co-prime, and thus typically $p_i(x)$ is taken to be the ith element in a list of monic irreducible polynomials over $\mathbb{F}_b$ sorted in non-decreasing order of degrees, so as to obtain the best possible t. This implies that Niederreiter sequences in base 2 are known to be (t,s)-sequences with a value of t smaller than the one that works for Sobol' sequences. Note, however, that the expression $\sum_{i=1}^{s}(e_i - 1)$ is an upper bound on t, and thus it is possible that the construction obtained is a (t^*, s)-sequence for $t^* < t$. The smallest such value of t^* is often referred to as the "exact t". Conditions under which $t = \sum_{i=1}^{s}(e_i - 1)$ is exact are given in [3].

2.4. The framework of Tezuka. The next and last family of constructions that is of relevance to this work is the one introduced by Tezuka [20], also discussed more comprehensively in [21]. Here we follow the framework given in [21] to describe this construction, which is called *generalized Niederreiter sequences* by Tezuka. The way in which it generalizes the construction discussed in Section 2.3 is that (2.3) is replaced by the expansion

$$\frac{y_{i,k}(x)}{p_i(x)^j} = \sum_{r=w}^{\infty} a^{(i)}(j,k,r) x^{-r},$$

where $1 \le i \le s$, $j, k \ge 1$, and the polynomials $y_{i,k}(x)$ must be chosen so that the (residue) polynomials $y_{i,k}(x) \bmod p_i(x)$ for $(j-1)e_i \le k-1 < je_i$ are linearly independent over $\mathbb{F}_b$. The generating matrices $C^{(i)}$ are then obtained as

$$c_{k,r}^{(i)} = a^{(i)}(q_i + 1, k, r),$$

where $q_i = \lfloor (k-1)/e_i \rfloor$.

Following [21, Remark 4], we note that for Niederreiter sequences, we have $y_{i,k}(x) = x^u g_{i,j}(x)$, where u and j satisfy $k - 1 = (j-1)e_i + u$ with $0 \le u < e_i$.

For the Sobol' sequences [21, Remark 2], and as explained in Section 2.1, the direction numbers determine the $e_i \times e_i$ direction (sub)matrix $D^{(i)}$ of $C^{(i)}$, and thus correspond to choosing certain polynomials $y_{i,1}(x), \ldots, y_{i,e_i}(x)$ that will be described in Section 4, more precisely in Theorem 4.4. We note that having $v_{r,r}^{(i)} = 1$ for $r = 1, \ldots, e_i$ implies that $y_{i,r}$ is of degree $e_i - r$ for $1 \le r \le e_i$, and thus the linear independence property mentioned above is satisfied (of course, this fundamental property is proved by Sobol' [19] in another way).

3. Sobol' and Niederreiter sequences in base 2

3.1. A founding example. We consider the first non-trivial primitive polynomial $p(x) = x^2 + x + 1$ corresponding to the monocyclic linear operator $u_{i+2} + u_{i+1} + u_i$ of order 2 in [19] (the monocyclic operator of the first order corresponds to the Pascal matrix modulo 2).

In the framework of Sobol', we consider the matrix associated with p, with starting direction numbers $(1, 3)$, resulting from the recurrence relation $V_{i+2} = V_{i+1} + V_i + V_i/4$ on column vectors (see [19, Section 3.2]).

In the framework of Niederreiter, we consider the matrix associated with p, generated row-by-row by the formal Laurent series $x^k/p(x)^j$, $0 \le k < 2$ (see [15, Section 6]).

A simple examination of these two matrices shows they are the same after permutation of odd and even rows of one of them. Details are shown in Figure 1. Also, it is easy to check for these two matrices that the recurrence relation of Sobol' applies to the Niederreiter matrix. In other words, taking $x^{1-k}/p(x)^j$ $(0 \le k < 2)$ in equation (2.3) gives the Sobol' matrix above. As mentioned before, the Sobol' matrices are NUT and therefore they generate $(0, 1)$-sequences. This is an advantage since there is no "leading-zeros phenomenon" (see [2, Section 3.3]) for Sobol' sequences. Another advantage for implementation is that there is only one recurrence relation for the whole Sobol' matrix instead of a recurrence relation for each odd row of a

Niederreiter matrix in base 2. Hence the interest of a generalization of our example.

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & \dots \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & \dots \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & \dots \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & \dots \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & \dots \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

Fig. 1. Generating matrices based on $p(x) = x^2 + x + 1$ for: Sobol' sequence with starting direction numbers $(1, 3)$ (left); Niederreiter sequence based on $g_{i,j} = 1$ (right).

3.2. Generalization

LEMMA 3.1 (Fundamental lemma for base 2). *The matrix of a Niederreiter sequence in base* 2 *generated by the formal Laurent series* $x^k/p(x)^j$ *(for* $0 \le k < e$ *and* $j \ge 1$*), where* p *is an irreducible polynomial of degree* e*, satisfies a Sobol' recurrence relation associated with* p*.*

Proof. We only consider irreducible polynomials $p(x)$ of degree $e \ge 2$, since the case $e = 1$ concerns the van der Corput sequence and its image by the Pascal matrix for which the matrices coincide.

Let $p(x) = a_e x^e + a_{e-1}x^{e-1} + \cdots + a_1 x + a_0$, where $a_e = a_0 = 1$ (we keep a_e and a_0 for more clarity). Then

$$\frac{1}{p(x)} = \sum_{r=1}^{\infty} \frac{u_r}{x^r} = \sum_{r=e}^{\infty} \frac{u_r}{x^r}$$

with $u_1 = \cdots = u_{e-1} = 0$, $u_e = 1$ and $a_e u_{r+e} = a_0 u_r + \cdots + a_{e-1} u_{r+e-1}$ for all $r \ge 1$.

We say that the linear recurrence relation formally associated with p is the relation (where + means addition modulo 2)

$$V_{r+e} = \frac{1}{2^e} a_0 V_r + a_0 V_r + a_1 V_{r+1} + \cdots + a_{e-1} V_{r+e-1} = \frac{1}{2^e} a_0 V_r + \sum_{h=0}^{e-1} a_h V_{r+h}$$

for all $r \ge 1$, where V_r is the rth column of the generating matrix associated with p in the framework of Sobol' (see Section 2.1). Of course, in the case where p is primitive, this relation coincides with equation (2.1).

Our goal is to prove that the matrix generated by the formal series $x^k/p(x)^j$ in the framework of Niederreiter satisfies such a relation. To this end, we establish the link between $1/p(x)^j$ and $1/p(x)^{j+1}$ thanks to the

product of the formal series $1/p(x)^j$ and $1/p(x)$. Set

$$\frac{1}{p(x)^j} = \sum_{r=1}^{\infty} \frac{v_r}{x^r} = \sum_{r=ej}^{\infty} \frac{v_r}{x^r} \quad \text{and} \quad \frac{1}{p(x)^{j+1}} = \sum_{r=1}^{\infty} \frac{w_r}{x^r} = \sum_{r=ej+e}^{\infty} \frac{w_r}{x^r}.$$

Then, for $r \geq ej + e$,

$$w_r = u_e v_{r-e} + u_{e+1} v_{r-e-1} + \cdots + u_{r-ej} v_{ej} = \sum_{l=e}^{r-ej} u_l v_{r-l}.$$

Hence, our objective is to prove the following linear recursion for the entries w_r of the $e(j+1)$th row in relation with the entries of the ejth row (for the remaining rows the property will follow from multiplication by the successive powers of x):

$$\Sigma := a_0 w_r + \cdots + a_e w_{r+e} = \sum_{f=0}^{e} a_f w_{r+f} = v_r \quad \text{for all } r \geq 1.$$

To this end, for $r \geq ej + e$, we collect the summands in Σ according to the factors v_l for $ej \leq l \leq r$:

$$\begin{aligned}\Sigma = {} & a_e u_e v_r + (a_{e-1} u_e + a_e u_{e+1}) v_{r-1} + (a_{e-2} u_e + a_{e-1} u_{e+1} + a_e u_{e+2}) v_{r-2} \\ & + \cdots + (a_0 u_{r-ej} + a_1 u_{r+1-ej} + \cdots + a_e u_{r+e-ej}) v_{ej}.\end{aligned}$$

Now we observe that all factors corresponding to $v_{r-1}, v_{r-2}, \ldots, v_{ej}$ are nought since they correspond to the recurrence relation in the expansion of $p(x)^{-1}$. ∎

In the case of primitive polynomials, Lemma 3.1 gives rise to the following generalization of the example in §3.1:

THEOREM 3.2. *After reordering the rows to get NUT matrices, Niederreiter sequences in base* 2 *generated by the formal series* $x^k/p_i(x)^j$, *where* p_i, $1 \leq i \leq s$, *are distinct primitive polynomials, are Sobol' sequences associated with the polynomials* p_i.

3.3. A further example with a non-primitive polynomial. We consider here $p(x) = x^4 + x^3 + x^2 + x + 1$, a non-primitive irreducible polynomial of degree 4. The recurrence relations to expand the formal series in the framework of Niederreiter are $v_{r+4} = v_{r+3} + v_{r+2} + v_{r+1} + v_r$ for the first row, $v_{r+8} = v_{r+6} + v_{r+4} + v_{r+2} + v_r$ for the row of rank 5, and so on. The linear (non-monocyclic) operator in the framework of Sobol' is $V_{i+4} = V_{i+3} + V_{i+2} + V_{i+1} + V_i + V_i/16$. The NUT matrix resulting from the permutation of rows of the Niederreiter matrix generated by $x^k/(p(x)^j$ (for $0 \leq k < 4$) is equal to a Sobol' type matrix with starting direction numbers $(1, 3, 3, 3)$ and the linear operator above. This relation is also satisfied by the Niederreiter matrix according to Lemma 3.1, and can easily be checked

on the matrices, as illustrated in Figure 2. But formally, we cannot speak of Sobol' matrices and sequences since the latter are only defined for primitive polynomials in base 2.

$$\begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \dots \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & \dots \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & \dots \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & \dots \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & \dots \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \dots \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \dots \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{bmatrix}
\qquad
\begin{bmatrix}
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & \dots \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & \dots \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & \dots \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \dots \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \dots \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \dots \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \dots \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{bmatrix}$$

Fig. 2. Generating matrices based on $p(x) = x^4 + x^3 + x^2 + x + 1$ for: Sobol' sequence with starting direction numbers $(1, 3, 3, 3)$ (left); Niederreiter sequence based on $g_{i,j} = 1$ (right).

4. Irreducible Sobol' sequences in prime power bases

4.1. Definition and generalization of Theorem 3.2. Here is the natural extension of the original Sobol' sequences in base 2 with primitive polynomials to arbitrary prime power bases and with monic irreducible polynomials.

Definition 4.1. Let $p(x) = x^e - a_{e-1}x^{e-1} - \cdots - a_1 x - a_0$ be a monic irreducible polynomial of degree e over $\mathbb{F}_b$, where b is a prime power. Define a generating matrix C associated with p by the linear recurrence relation

$$V_{r+e} - a_{e-1}V_{r+e-1} - \cdots - a_1 V_{r+1} - a_0 V_r = \frac{1}{b^e} V_r, \tag{4.1}$$

where V_r $(r \geq 1)$ is the rth column of C, and with e starting direction numbers $d_1, \dots, d_e$ $(1 \leq d_r < b^r$ with $\gcd(d_r, b) = 1)$ defining an NUT $e \times e$ direction matrix D for C (see Section 2.1). Then, according to the general principle of construction, an s-dimensional *irreducible Sobol' sequence* is obtained from s different monic irreducible polynomials p_i generating s such matrices $C^{(i)}$ (typically, one chooses the first s ones in a list of all monic irreducible polynomials sorted according to non-decreasing degree, as is done for Niederreiter sequences). For short, we will often refer to irreducible Sobol' sequences as *IS-sequences*. Note that when working in a general prime power base b, one also needs to choose bijections ψ_r and $\lambda_{i,j}$ to go back and forth

between $\mathbb{F}_b$ and $\mathbb{Z}_b$ so that points in $[0,1)$ can then be defined (see the definition of the digital method in Section 1).

By construction, the generating matrices of irreducible Sobol' sequences are NUT, so that their one-dimensional projections are $(0,1)$-sequences. Also, it is worth noting that no truncation is required in their definition (in contrast with other types of low-discrepancy sequences).

Further, we point out that column-by-column constructions other than (2.1) and our proposed generalization (4.1) have been used elsewhere. Namely, Hofer [7] and Hofer and Niederreiter [8] have recently introduced different families of low-discrepancy sequences that also use this principle to construct their underlying generating matrices. However, the nature of their constructions is quite different; in particular, the columns are not defined through a recursive relation based on a given polynomial as in (2.1) and (4.1).

Next, we prove the analog of Lemma 3.1 for irreducible Sobol' sequences in prime power bases. Then, we show their close relation with the class of Niederreiter sequences generated by formal Laurent series of the form $x^k/p_i(x)^j$, i.e., Niederreiter sequences whose polynomials are $g_{i,j} = 1$ (this is the class for which Dick and Niederreiter determine the exact t-value in [3, Section 3]).

LEMMA 4.2 (Fundamental lemma for prime power base b). *The matrix of a Niederreiter sequence in prime power base b generated by the formal Laurent series $x^k/p(x)^j$ (for $0 \le k < e$ and $j \ge 1$), where p is a monic irreducible polynomial over $\mathbb{F}_b$ with* $\deg(p) = e$, *satisfies the Sobol' recurrence relation* (4.1) *associated with p.*

Proof. First, as was noted in the proof of Lemma 3.1 (the case $b = 2$), we only need to consider polynomials of degree $e \ge 2$.

Let $p(x) = x^e - a_{e-1}x^{e-1} - \cdots - a_1 x - a_0$ (we adopt the notation of Niederreiter as in [15, Section 6]). Then

$$\frac{1}{p(x)} = \sum_{r=1}^{\infty} \frac{u_r}{x^r} = \sum_{r=e}^{\infty} \frac{u_r}{x^r} \tag{4.2}$$

with $u_1 = \cdots = u_{e-1} = 0$, $u_e = 1$ and $a_e u_{r+e} = a_0 u_r + \cdots + a_{e-1} u_{r+e-1}$ for all $r \ge 1$. For $b = 2$, we recover the expression for p in the proof of Lemma 3.1 (since $-1 = 1$ in $\mathbb{F}_2$).

We first recall the link established in that proof between $1/p(x)^j$ and $1/p(x)^{j+1}$ (thanks to the product of the series $1/p(x)^j$ and $1/p(x)$): with

$$\frac{1}{p(x)^j} = \sum_{r=1}^{\infty} \frac{v_r}{x^r} = \sum_{r=ej}^{\infty} \frac{v_r}{x^r} \quad \text{and} \quad \frac{1}{p(x)^{j+1}} = \sum_{r=1}^{\infty} \frac{w_r}{x^r} = \sum_{r=ej+e}^{\infty} \frac{w_r}{x^r}$$

for $r \ge ej + e$, we have $w_r = u_e v_{r-e} + u_{e+1} v_{r-e-1} + \cdots + u_{r-ej} v_{ej} = \sum_{l=e}^{r-ej} u_l v_{r-l}$.

According to the form of the linear recurrence relation (4.1), we have to prove that for $r \geq 1$ (see the proof of Lemma 3.1 for more details),

$$\Sigma := w_{r+e} - a_{e-1}w_{r+e-1} - \cdots - a_1 w_{r+1} - a_0 w_r = w_{r+e} - \sum_{f=0}^{e-1} a_f w_{r+f} = v_r.$$

To this end, for $r \geq ej + e$, we collect the summands in Σ according to the factors v_l for $ej \leq l \leq r$:

$$\begin{aligned}\Sigma = {} & u_e v_r + (u_{e+1} - a_{e-1}u_e)v_{r-1} + (u_{e+2} - a_{e-1}u_{e+1} - a_{e-2}u_e)v_{r-2} \\ & + \cdots + (u_{r+e-ej} - a_{e-1}u_{r+e-1-ej} - \cdots - a_1 u_{r+1-ej} - a_0 u_{r-ej})v_{ej}.\end{aligned}$$

Now we observe that all factors corresponding to $v_{r-1}, v_{r-2}, \ldots, v_{ej}$ are nought, since they correspond to the recurrence relation in the expansion of $p(x)^{-1}$. ∎

As announced earlier, we can now provide the analog of Theorem 3.2, adapted to the more general context of this section.

THEOREM 4.3. *After reordering the rows to get NUT matrices, Niederreiter sequences in a prime power base b generated by the formal Laurent series $x^k/p_i(x)^j$, where p_i, $1 \leq i \leq s$, are distinct monic irreducible polynomials, are IS-sequences associated with the polynomials p_i.*

4.2. Characterization within the family of generalized Niederreiter sequences. In this section, we study the connections between irreducible Sobol' sequences and generalized Niederreiter sequences, starting with the following result.

THEOREM 4.4 (Membership property). *Irreducible Sobol' sequences in a prime power base are generalized Niederreiter sequences (in the framework of Tezuka) in which the polynomials p_i are distinct monic irreducible polynomials and the polynomials $y_{i,k}$ equal $y_{i,h}$, where $\deg(y_{i,h}) = e_i - h$ and $h = k - 1 \bmod e_i + 1$. More precisely, the polynomials $y_{i,h}$ are given by the polynomial part of $p_i(x)(v_{h,h}^{(i)}x^{-h} + v_{h,h+1}^{(i)}x^{-(h+1)} + \cdots + v_{h,e}^{(i)}x^{-e})$, where the $v_{h,l}^{(i)}$ for $1 \leq h, l \leq e_i$ are the entries of the direction matrix $D^{(i)}$, $1 \leq i \leq s$.*

Conversely, in the next result, we identify which generalized Niederreiter sequences are irreducible Sobol' sequences. To do so, we make use of the matrix of direction numbers

$$D_{gN}^{(i)} = \begin{bmatrix} u_e^{(i)} & u_{e+1}^{(i)} & \cdots & u_{2e-1}^{(i)} \\ 0 & u_e^{(i)} & \ddots & u_{2e-2}^{(i)} \\ 0 & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & u_e^{(i)} \end{bmatrix}, \tag{4.3}$$

where the $u_r^{(i)}$ come from the expansion of $1/p_i(x)$ as in (4.2). (When we write D_{gN} without the superscript i, we refer to the matrix (4.3) associated with the coefficients of $1/p(x)$.)

Note that the IS-sequences mentioned in Theorem 4.3 are based on direction matrices given precisely by $D_{gN}^{(i)}$ for $1 \le i \le s$.

THEOREM 4.5. *Generalized Niederreiter sequences (in the framework of Tezuka) in a prime power base in which the polynomials p_i are distinct monic irreducible polynomials and the polynomials $y_{i,k}$ equal $y_{i,h}$, where* $\deg(y_{i,h}) = e_i - h$ *and* $h = k - 1 \bmod e_i + 1$, *are irreducible Sobol' sequences based on the polynomials p_i and direction matrices $D^{(i)} = Y^{(i)} D_{gN}^{(i)}$, where the (l,r)th entry of $Y^{(i)}$ is given by the coefficient of x^{e-r} in $y_{i,l}(x)$, $1 \le l, r \le e_i$.*

REMARK 4.6. In his book [21, Definition 6.6], Tezuka gives a definition of what he calls *generalized Sobol' sequences in base $b = 2$* as a special case of his definition of generalized Niederreiter sequences in which all mappings $\lambda_{i,j}$ and ψ_r are identity mappings and the polynomial p_i is the ith irreducible polynomial in a list of all irreducible polynomials in base 2 sorted according to non-decreasing degree. But curiously, he does not require any condition on the polynomials $y_{i,k}$, as he did in his interpretation of Sobol' sequences in his framework [21, Remark 2] where our condition above is mentioned.

In order to prove Theorems 4.4 and 4.5, we use the following two technical lemmas, which help understand the relation between different IS-sequences and different generalized Niederreiter sequences, respectively.

LEMMA 4.7. *Consider an IS-sequence in prime power base b based on the monic irreducible polynomial p of degree e and with $e \times e$ direction matrix D. Consider the IS-sequence also based on p but with a direction matrix given by the identity matrix. Let their generating matrices be denoted by C_D and C_I, respectively. Then $C_D = AC_I$, where A is a block diagonal matrix with $e \times e$ blocks given by D.*

LEMMA 4.8. *Consider a generalized Niederreiter sequence in a prime power base b based on the monic irreducible polynomial p of degree e and generated by the polynomials $y_k(x) = x^{e-h}$, where $h = k - 1 \bmod e + 1$, for $k \ge 1$. Let its generating matrix be denoted by C_{gN}. Consider another generalized Niederreiter sequence in base b based on the same monic irreducible polynomial p, but generated by polynomials $y_k(x)$ such that $y_k(x)$ is of degree $e - h$ for $k \ge 1$, with h defined as above. Let its generating matrix be denoted by C. Then $C = AC_{gN}$, where A is a block diagonal matrix with blocks A_j of size $e \times e$ and (h,r)th entry given by the coefficient of x^{e-r} in $y_k(x)$, where $(k-1) = (j-1)e + (h-1)$.*

Lemma 4.8 is straightforward once we observe that each polynomial $y_k(x)$ associated to C is a linear combination of the polynomials $\{1, x, \ldots, x^{e-1}\}$ that are associated with the matrix C_{gN}, and therefore the expansion of $y_k(x)/(p_i(x)^j)$ is obtained by taking an appropriate combination of the rows of the jth block of C_{gN}. Lemma 4.7 is closely related to [13, Proposition 2], except that the latter is for a Sobol' sequence in base 2 based on primitive polynomials. However, the proof given there rests on the fact that the corresponding generating matrix is built on a recurrence of the form (4.1), and hence can be easily adapted to the case of a prime power base and a monic irreducible polynomial, as shown below.

Proof of Lemma 4.7. We first define the matrices

$$Q = \begin{pmatrix} a_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ a_{e-1} & \cdots & a_1 & a_0 \end{pmatrix}$$

and R_k, which is an $e \times e$ matrix with zeros everywhere except in the first $k-1$ entries of the kth column, given by $a_{e-(k-1)}, \ldots, a_{e-1}$. We also define

$$F = (I + R_2) \cdots (I + R_e),$$

where I is the $e \times e$ identity matrix. Finally, we split the generating matrix C_D into blocks $B_{l,r}$ of size $e \times e$, in such a way that

$$C = \begin{pmatrix} B_{1,1} & B_{1,2} & B_{1,3} & \cdots \\ 0 & B_{2,2} & B_{2,3} & \cdots \\ 0 & 0 & B_{3,3} & \cdots \\ \vdots & \ddots & \ddots & \ddots \end{pmatrix},$$

where the 0's indicate an $e \times e$ zero matrix, i.e., $B_{l,r}$ is the zero matrix when $l > r$. The main ingredient of the proof is to observe that (4.1) implies that the blocks are updated recursively using

(4.4)
$$B_{1,r} = B_{1,r-1}QF \quad \text{for } r > 1, \qquad B_{l,r} = (B_{l,r-1}Q + B_{l-1,r-1})F \quad \text{for } l, r > 1,$$

with $B_{1,1} = D$ as a starting matrix (which leads to $B_{l,l} = DF^{l-1}$ as the starting matrix for the lth row of blocks).

To see why this holds, first consider the case $l = 1$. The (j, c)th entry of $B_{1,r}$ is obtained by first taking the product of the jth row of $B_{1,r-1}$ by the vector containing $c-1$ zeros followed by $a_0, \ldots, a_{e-c}$, which is precisely what the multiplication by Q achieves. To this product, we must then add a_{e-c+1} times the first entry in the jth row of $B_{1,r-1}Q$, plus a_{e-c+2} times the

second (updated) entry in that same row, up until a_{e-1} times the $(c-1)$th (updated) entry in that row. This is done via multiplication by $I + R_c$. But first we need to perform successive multiplications of $B_{1,r-1}Q$ by $I + R_l$ for $l = 2, \ldots, c-1$ to ensure the previous elements of the row are updated. Multiplication by $I + R_l$ for $l > c$ has no effect on entry (j, c).

The case $l > 1$ is obtained similarly, but before applying F—which, as we just saw, has the effect of adding the terms that come from the current block itself—we must add to $B_{l,r-1}Q$ the block $B_{l-1,r-1}$ corresponding to the term V_r/b^e in (4.1).

The recursions given in (4.4) show that each block has the form $B_{l,r} = DH_{l,r}$ where $H_{l,r}$ does not depend on D. Observing that C_I is made up of the blocks $H_{l,r}$ yields the desired result. ∎

We can now prove the two preceding theorems. In both cases, we show the result for a given dimension i and drop the index i to ease the presentation. Also, both results make use of the direction matrix D_{gN} given in (4.3).

Proof of Theorem 4.4. From Theorem 4.3 we can see that the generating matrix of an IS-sequence based on the direction matrix D_{gN} is equal to the generating matrix of a generalized Niederreiter sequence based on the polynomials $y_k(x) = x^{e-h}$ for $k \geq 1$, where $h = k - 1 \bmod e + 1$. Denote this common generating matrix by C_{gN}.

Then, Lemma 4.7 shows that the generating matrix C of an IS-sequence based on a general direction matrix D is related to C_{gN} via the relation $C = AC_{gN}$, where A is the block diagonal matrix with a common NUT $e \times e$ block matrix A_D given by $A_D = D \cdot D_{gN}^{-1}$.

Next we need to show that the matrix C corresponds to a generalized Niederreiter sequence, but this follows from Lemma 4.8, which implies that the generalized Niederreiter sequence based on the polynomials $y_k(x) = a_h(x)$ where $a_h(x) = a_{h,h}x^{e-h} + a_{h,h+1}x^{e-h-1} + \cdots + a_{h,e}$ for $1 \leq h \leq e$, and where $a_{h,l}$ is the entry on the hth row and lth column of A_D, has a generating matrix given precisely by AC_{gN}.

The last step is to show that these polynomials $a_h(x)$ are in fact given by the polynomial part of $p(x)(v_{h,h}x^{-h} + v_{h,h+1}x^{-(h+1)} + \cdots + v_{h,e}x^{-e})$, which we denote as $y_h(x)$ for $1 \leq h \leq e$, and where the $v_{h,l}$ are the entries of the direction matrix D. In other words, we want to show that the rows of the matrix $A_D = DD_{gN}^{-1}$ are given by

$$A_h = (0, \ldots, 0, y_{h,e-h}, y_{h,e-h-1}, \ldots, y_{h,0}) \quad \text{for } 1 \leq h \leq e, \tag{4.5}$$

where the $y_{h,l}$ are such that $y_h(x) = y_{h,e-h}x^{e-h} + y_{h,e-h-1}x^{e-h-1} + \cdots + y_0$. We actually show instead the equivalent statement that the matrix A_D defined by (4.5) satisfies $A_D D_{gN} = D$. Obserwe that by definition of $y_h(x)$,

$$y_{h,e-l} = v_{h,l} - a_{e-1}v_{h,l+1} - \cdots - a_{e-(l-h)}v_{h,h} \quad \text{for } h \leq l \leq e. \tag{4.6}$$

Now, to establish that $A_D D_{gN} = D$, we must prove

$$(4.7)\qquad (0,\dots,0,y_{h,e-h},y_{h,e-h-1},\dots,y_{h,0}) \cdot (u_{e+l-1},u_{e+l-2},\dots,u_e,0,\dots,0) = v_{h,l}$$

for $1 \le h,l \le e$. We first note that if $l < h$, then both sides of (4.7) are 0. If $l \ge h$, then we replace each $y_{h,l}$ on the left-hand-side of (4.7) by its definition given in (4.6). Hence we get

$$\begin{aligned}(4.8)\qquad & u_{e+l-h}v_{h,h} + u_{e+l-h-1}(v_{h,h+1} - a_{e-1}v_{h,h}) \\ &\quad + \cdots + u_e(v_{h,l} - a_{e-1}v_{h,l-1} - \cdots - a_{e-(l-h)}v_{h,h}) \\ &= v_{h,h}(u_{e+l-h} - a_{e-1}u_{e+l-h-1} - \cdots - a_{e-(l-h)}u_e) \\ &\quad + v_{h,h+1}(u_{e+l-h-1} - a_{e-1}u_{e+l-h-2} - \cdots - a_{e-(l-h-1)}u_e) \\ &\quad + \cdots + v_{h,l-1}(u_{e+1} - a_{e-1}u_e) + v_{h,l}u_e = v_{h,l},\end{aligned}$$

since in (4.8) the term multiplying $v_{h,i}$ for $h \le i < l$ is 0, by definition of the u_l's, while $v_{h,l}$ is multiplied by $u_e = 1$. ∎

Proof of Theorem 4.5. From Theorem 4.3, we can see that a generalized Niederreiter sequence based on $y_{i,k} = x^{e-h}$, where $h = k - 1 \bmod e + 1$, has the same generating matrix as an IS-sequence based on the direction matrix D_{gN}. Denote this common generating matrix by C_{gN}.

Next, we observe (from Lemma 4.8) that the generating matrix of a generalized Niederreiter sequence as in the statement is $C = AC_{gN}$, where A is a block diagonal matrix with blocks Y of size $e \times e$ given by

$$Y = \begin{bmatrix} y_{1,e-1} & y_{1,e-2} & \cdots & y_{1,0} \\ 0 & y_{2,e-2} & \cdots & y_{2,0} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & y_{e,0} \end{bmatrix},$$

where the $y_{h,l}$ come from the polynomials $y_h(x)$, i.e., $y_h(x) = y_{h,e-h}x^{e-h} + \cdots + y_{h,0}$ for $1 \le h \le e$. We thus need to show that C satisfies the conditions of an IS-sequence. This is achieved via Lemma 4.7, which implies that $C = AC_{gN}$ is an IS-sequence based on the direction matrix $D = YD_{gN}$. ∎

4.3. Discrepancy properties of irreducible Sobol' sequences. In this section, we collect the main properties of irreducible Sobol' sequences regarding discrepancy and resulting from the membership property stated in Theorem 4.4. We thus view them as corollaries of this result.

Corollary 4.9. *An IS-sequence in prime power base b based on distinct monic irreducible polynomials p_i of respective degrees e_i has the following properties:*

(1) *It is a digital* (t,s)*-sequence in base* b *with* $t=\sum_{i=1}^{s}(e_i-1)$.
(2) *Its discrepancy satisfies* (1.1) *with*

$$c_s=\begin{cases}\dfrac{b^t}{s!}\,\dfrac{b^2}{2(b^2-1)}\left(\dfrac{b-1}{2\log b}\right)^s & \text{if } b \text{ is even (from [5])},\\[2ex] \dfrac{b^t}{s!}\,\dfrac{1}{2}\left(\dfrac{b-1}{2\log b}\right)^s & \text{if } b \text{ is odd (from [12])}.\end{cases}$$

(3) *In the framework introduced in* [22]*, it is also a* $(0,\mathbf{e},s)$*-sequence in base* b *with* $\mathbf{e}=(e_1,\dots,e_s)$.
(4) *Its discrepancy also satisfies* (1.1) *with*

$$c_s=\frac{1}{s!}\prod_{i=1}^{s}\frac{b^{e_i}-1}{2e_i\log b}\quad (\text{from [22] for } b \text{ odd and [6] for } b \text{ even}).$$

As mentioned above, once we have the membership property given in Theorem 4.4, the above properties follow from known results on generalized Niederreiter sequences. More precisely, property (1) follows from [21, Thm. 6.3 and Lemma 6.1], while property (3) follows directly from [22, Thm. 1]. Once we have these two properties, we simply recall the best known discrepancy bounds for (t,s) and $(0,\mathbf{e},s)$-sequences in properties (2) and (4), respectively.

It is worth mentioning that in base 2, the expression for c_s obtained from the $(0,\mathbf{e},s)$-sequence representation of an IS-sequence (given in property (4) above) is shown to satisfy $c_s=O(1/(s(2\log 2)^s))$ in [22, p. 246], which goes to 0 with s. The proof relies on a result of Pollack [18] on the prime number theorem for polynomials over a finite field, combined with Atanassov's approach to studying the constant c_s for Halton sequences. Since this result requires the underlying sequence to be based on a list of all irreducible polynomials over $\mathbb{F}_2$ sorted by non-decreasing degree, it holds for IS-sequences, but not for the original Sobol' sequences. For the latter, based on the bound given in property (2) above and the known behaviour of t as a function of s for these sequences, the constant c_s instead goes to infinity with s.

5. Niederreiter sequences compared to Sobol' sequences in prime power base. In this section, our aim is to investigate which Niederreiter sequences (with $g_{i,j}=g_i$ for all $j\geq 1$) are IS-sequences after reordering of the rows of their generating matrices, so as to situate these two families of generalized Niederreiter sequences in the framework of Tezuka.

First, we proceed to a direct study to find which necessary conditions a Niederreiter sequence has to satisfy to be an IS-sequence. Then, we will give a characterization of such sequences.

Our first observation is that a Niederreiter sequence based on a monic irreducible polynomial p with $\deg(p)=e$ can be an IS-sequence only if there

exists a polynomial $z(x) \in \mathbb{F}_b[x]/(p(x))$ such that $\{z(x), xz(x), \ldots, x^{e-1}z(x)\}$ has exactly one polynomial of degree l for $0 \le l < e$ (see the definitions of Niederreiter sequences and IS-sequences). Such a polynomial $z(x)$ then becomes a candidate for $g_i(x)$.

So, we first need a polynomial of degree 0 in the above set, which implies the only possible polynomials z are the inverses of powers of x in $\mathbb{F}_b[x]/(p(x))$. In order to determine these inverses, we observe that the polynomial (where $p(x) = x^e - a_{e-1}x^{e-1} - \cdots - a_1x - a_0$)

$$g(x) = (p(x) + a_0)/x = x^{e-1} - a_{e-1}x^{e-2} - \cdots - a_2x - a_1$$

is the inverse of x/a_0, so that g^l is the inverse of $(x/a_0)^l$ for $0 \le l < e$. Therefore $g^0 = 1, g, \ldots, g^{e-1}$ are the only polynomials among the 2^e polynomials in $\mathbb{F}_b[x]/(p(x))$ that can be suitable. Notice that the case $e = 1$ is trivial (in this case, the generating matrices are the powers of the Pascal matrix for both families), hence from now on we take $e \ge 2$.

Next, we have to deal with the condition on the degrees, which (as we are going to see) involves the coefficients of p. We already have the degrees 0 and $e-1$ with g^0 and g. For the other powers of g, we consider the polynomials p from binomials to the general case where, for some $0 < m < e$, $a_m \ne 0$.

• First let $p(x) = x^e - a_0$. In this case $g(x) = x^{e-1}$, so $g^l(x) = a_0^{l-1}x^{e-l}$ for $0 < l < e$, and hence all powers of g are suitable (notice that this case does not occur if $b = 2$).

• Next let $p(x) = x^e - a_{e-1}x^{e-1} - a_0$ with $a_{e-1} \ne 0$. In this case, $g(x) = x^{e-1} - a_{e-1}x^{e-2}$, so $g^l(x) = a_0^l/x^l = (a_0^{l-1}/x^{l-1})g(x) = a_0^{l-1}x^{e-l-1}(x - a_{e-1})$, and hence $\deg(g^l) = e - l$ for $1 < l < e-1$. Here also we find that all powers of g from 0 to $e-1$ are suitable.

• Further, suppose $p(x) = x^e - a_{e-1}x^{e-1} - \cdots - a_fx^f - a_0$ with $a_f \ne 0$ $(1 \le f < e-1)$. In this case,

$$g(x) = x^{e-1} - a_{e-1}x^{e-2} - \cdots - a_fx^{f-1} = x^{f-1}(x^{e-f} - \cdots - a_{f+1}x - a_f).$$

Hence, $g^l(x) = a_0^l/x^l = (a_0^{l-1}/x^{l-1})g(x) = a_0^{l-1}x^{f-l}(x^{e-f} - \cdots - a_0)$ for $0 < l \le f$, so that $\deg(g^l) = e - l$ for $0 < l \le f$. But

$$g^{f+1} = g^f g = a_0^{f-1}(x^{e-f} - \cdots - a_0)a_0/x = a_0^f(x^{e-f-1} - \cdots - a_{f+1} - g(x)).$$

Thus $\deg(g^{f+1}) = \deg(g) = e - 1$, which implies that g^{f+1} does not satisfy the condition on the degrees since we have already selected g. And so neither do the next powers of g because multiplication by powers of x still reintroduces g to the list (indeed, for $f+1 < l < e$, we have $g(x) = x^{l-1}g^l(x)$). We conclude that when $a_f \ne 0$ there are exactly $f + 1$ polynomials satisfying the condition on the degrees: $g^0, g, \ldots, g^f$. In the end, if $a_1 \ne 0$, i.e., $f = 1$, we only have the two polynomials we found when starting the process: g^0 and g.

From the preceding direct study, we are now in a position to state the following characterization.

THEOREM 5.1. *Let $p(x) = x^e - a_{e-1}x^{e-1} - \cdots - a_1 x - a_0$ be a monic irreducible polynomial over $\mathbb{F}_b$ where b is a prime power base. The polynomials $z \in \mathbb{F}_b[x]/(p(x))$ such that $\{x^k z(x)/p(x) : k = 0, \ldots, e-1\}$ generates an $e \times e$ NUT matrix are the polynomials $g^0, g, \ldots, g^f$ where $g(x) = (p(x) + a_0)/x$ and where f is the least positive index satisfying $a_f \neq 0$.*

Proof. The direct part follows from the observations above. Conversely, suppose that f is the least positive index for which $a_f \neq 0$. Then $p(x) = x^f h(x) - a_0$ with $\deg(h) = e - f$ and $h(0) \neq 0$, so that $g(x) = a_0/x = x^{f-1}h(x)$ and $g^l(x) = a_0^{l-1}x^{f-l}h(x)$. Hence, $\deg(g^l) = e - l$ for $1 \leq l \leq f$. Moreover, $g^{f+1} = a_0^f h(x)/x$, which implies that $\deg(g^{f+1}) = \deg(g)$ (since $h(0)/x = g(x)h(0)/a_0$) and the same holds for the next powers of g. Thus we have shown that $z(x) \in \mathbb{F}_b[x]/(p(x))$ of the form $g^0, g, \ldots, g^f$ is such that $x^k z(x)/p(x)$ generates an NUT matrix (but not the next powers of g). ∎

Using the characterization provided in Theorem 5.1, we can now determine which Niederreiter sequences are also IS-sequences. It turns out that the only ones are those based on $g_{i,j}(x) = 1$ for all i and j. The other polynomials g found in Theorem 5.1 do not yield IS-sequences because, although they provide an NUT matrix for the upper left $e \times e$ block of the generating matrix, this property does not hold on the following blocks, as shown in the proof of the next result.

THEOREM 5.2. *The only Niederreiter sequences in a prime power base b that are IS-sequences (after reordering the rows to get NUT matrices) are those based on $g_{i,j}(x) = 1$ for all $i = 1, \ldots, s$ and $j \geq 1$.*

Proof. From Theorem 4.2, we already know that taking $g_{i,j} = 1$ yields an IS-sequence. Drop the subscript i and focus on a given coordinate based on a monic irreducible polynomial p; what remains to be proved is that taking $g_j(x) = g^l(x)$ with $1 \leq l \leq f$ for all $j \geq 1$, with $g(x)$ and f as described in Theorem 5.1, does not yield an NUT matrix.

By definition, $g^l(x)$ is of degree $e - l$. Thus the expansion of $g^l(x)/p^2(x)$ has a non-zero coefficient for x^{-e-l}. This implies that the expansion of $x^k g^l(x)/(p^2(x))$ has a non-zero coefficient for $x^{-(e+l-k)}$ and $e + l - k \leq e$ when $k \geq l$, which is a valid value for k since it runs from 0 to $e - 1$ and $1 \leq l \leq e - 1$. Since we have a non-zero coefficient in one of the first e columns and on a row with rank larger than e, the corresponding matrix is not NUT. ∎

From the proof of Theorem 5.2, we can see more precisely why we do not get an NUT matrix when $g_{i,j} \neq 1$: the problem is that in the definition of Niederreiter sequences, rows are obtained using the expansion of

$x^k g_{i,j}(x)/p^j(x)$, where polynomials are multiplied in $\mathbb{F}_b[x]$ in the numerator rather than in $\mathbb{F}_b[x]/p(x)$. Since this yields numerators with degrees larger than $e-1$, when dividing by $p^j(x)$ with $j>1$, we obtain non-zero coefficients to the left of the diagonal. This suggests a simple modification to the definition of Niederreiter sequences in order to allow for the existence of such sequences that are also IS-sequences, other than those generated by $g_{i,j}=1$, as we now describe.

Definition 5.3. A *reduced Niederreiter sequence* in a prime power base b is obtained by choosing s pairwise co-prime polynomials $p_1(x),\dots,p_s(x)\in\mathbb{F}_b[x]$ of respective degrees e_i, and a series of polynomials $g_{i,j}(x)\in\mathbb{F}_b[x]$ for $i=1,\dots,s$ and $j\geq 1$ such that $\gcd(g_{i,j}(x),p_i(x))=1$ for all i,j. The generating matrices are defined through their rows by first developing the formal Laurent series

$$\frac{x^k g_{i,j}(x) \bmod p_i(x)}{(p_i(x))^j}=\sum_{r=w}^{\infty} a^{(i)}(j,k,r)x^{-r-1}. \tag{5.1}$$

The elements of the generating matrices are then defined as

$$c_{j,r}^{(i)}=a^{(i)}(q_i+1,u,r-1),$$

where q_i and u depend on i and j through the relation $j-1=q_i e_i+u$ with $0\leq u\leq e_i-1$.

Hence a reduced Niederreiter sequence only differs from the original definition through the $\bmod p_i(x)$ operation applied to $x^k g_{i,j}(x)$ before dividing by $p_i^j(x)$ to get the formal Laurent series expansion. It thus belongs to the larger set of generalized Niederreiter sequences. With this simple modification, the characterization provided in Theorem 5.1 tells us which reduced Niederreiter sequences yield IS-sequences, as stated in the next result.

Theorem 5.4. *The only reduced Niederreiter sequences in a prime power base b that are IS-sequences (after reordering the rows to get NUT matrices) are those based on $g_{i,j}(x)=g_i(x)$, for all $i=1,\dots,s$ and $j\geq 1$, with g_i given by the characterization of Theorem* 5.1.

Proof. We consider a fixed dimension i and show the result is true for that coordinate, dropping the subscript i to simplify the notation. We also use $z_j(x)$ to represent a feasible polynomial for the jth block of rows, i.e., $z_j(x)$ is such that taking $g_{i,j}(x)=z_j(x)$ for $j\geq 1$ yields an IS-sequence on the ith coordinate.

We already know from Theorem 5.1 that $z_1(x)$ must be in $\{g^0,\dots,g^f\}$ in order for the NUT property to hold on the first e rows, where we recall that f is the least positive index such that $a_f\neq 0$ in $p(x)=x^e-a_{e-1}x^{e-1}-\cdots-a_1x-a_0$. What we need to establish is that taking $z_j(x)=z(x)$ for all $j\geq 1$, where $z(x)\in\{g^0,\dots,g^f\}$, is the only possible choice to get an

IS-sequence. But this follows directly from Theorem 4.4, which implies that a generalized Niederreiter sequence must satisfy the condition $y_{i,k} = y_{i,h}$ with $h = k - 1 \bmod e + 1$ for all $k \geq 1$ in order to be an IS-sequence. In the above setting, this can only happen if $z_j(x) = z(x)$ for all $j \geq 1$. ∎

6. Conclusion. In this paper, we have introduced a generalization of Sobol' sequences that preserves two key properties of this widely used construction, namely $(0, 1)$-sequences for each one-dimensional projection, and an easy-to-implement column-by-column construction for the generating matrices based on linear recurrences determined by monic irreducible polynomials over $\mathbb{F}_b$, where b is a prime power. Our generalization, which we call irreducible Sobol' (IS) sequences, is included in the very wide family of generalized Niederreiter sequences introduced by Tezuka [20], and we have shown precise connections between these two constructions. We have also shown that Niederreiter sequences and IS-sequences are quite different, as they intersect only for one specific choice of parameters, and after reordering the rows of the Niederreiter sequences to get NUT matrices.

An immediate item of interest for future work would be to search for good direction matrices for our proposed IS-sequences, initially for base 2 but for other prime power bases as well. A starting point to do so will be the implementation developed in [2] and its accompanying comparative study of different sequences. While in that work, the basic Niederreiter sequences (with $g_{i,j} = 1$) were seen to suffer from the leading-zeros phenomenon, this problem is avoided by IS-sequences by design, since they are based on NUT matrices. We thus expect that when tools to implement IS-sequences are developed and their performance in practice is assessed, their potential for use in quasi-Monte Carlo methods will become very clear.

Acknowledgments. We wish to thank Harald Niederreiter and Art Owen for their feedback on this paper. We also thank the anonymous referee for providing suggestions that helped us to improve the presentation. The second author's work was supported by NSERC (grant no. 238959).

References

[1] P. Bratley and B. L. Fox, *Algorithm 659: Implementing Sobol's quasirandom sequence generator*, ACM Trans. Math. Software 14 (1988), 88–100.

[2] P. Bratley, B. L. Fox, and H. Niederreiter, *Implementation and tests of low-discrepancy sequences*, ACM Trans. Model. Comput. Simul. 2 (1992), 195–213.

[3] J. Dick and H. Niederreiter, *On the exact t-value of Niederreiter and Sobol' sequences*, J. Complexity 24 (2008), 572–581.

[4] H. Faure, *Discrépance de suites associées à un système de numération (en dimension s)*, Acta Arith. 61 (1982), 337–351.

[5] H. Faure and P. Kritzer, *New star discrepancy bounds for* (t, m, s)*-nets and* (t, s)*-sequences*, Monatsh. Math. 172 (2013), 55–75.
[6] H. Faure and C. Lemieux, *A variant of Atanassov's method for* (t, s)*-sequences and* $(t, \mathbf{e}, s)$*-sequences*, J. Complexity 30 (2014), 620–633.
[7] R. Hofer, *A construction of low-discrepancy sequences involving finite-row digital* (t, s)*-sequences*, Monatsh. Math. 171, (2013), 77–89.
[8] R. Hofer and H. Niederreiter, *A construction of* (t, s)*-sequences with finite-row generating matrices using global function fields*, Finite Fields Appl. 21 (2013), 97–110.
[9] P. Jäckel, *Monte Carlo Methods in Finance*, Wiley, New York, (2002).
[10] S. Joe and F. Y. Kuo, *Remark on Algorithm 659: Implementing Sobol's quasirandom sequence generator*, ACM Trans. Math. Software 29 (2003), 49–57.
[11] S. Joe and F. Y. Kuo, *Constructing Sobol' sequences with better two-dimensional projections*, SIAM J. Sci. Comput. 30 (2008), 2635–2654.
[12] P. Kritzer, *Improved upper bounds on the star discrepancy of* (t, m, s)*-nets and* (t, s)*-sequences*, J. Complexity 22 (2006), 336–347.
[13] C. Lemieux and H. Faure, *New perspectives on* $(0, s)$*-sequences*, in: Monte Carlo and Quasi-Monte Carlo Methods 2008, P. L'Ecuyer and A. B. Owen (eds.), Springer, Heidelberg, 2009, 113–130.
[14] H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. 104 (1987), 273–337.
[15] H. Niederreiter, *Low-discrepancy and low-dispersion sequences*, J. Number Theory 30 (1988), 51–70.
[16] H. Niederreiter and C. P. Xing, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. 2 (1996), 241–273.
[17] H. Niederreiter and C. P. Xing, *Quasirandom points and global functions fields*, in: Finite Fields and Applications, S. Cohen and H. Niederreiter (eds.), London Math. Soc. Lectures Note Ser. 233, Cambridge Univ. Press, Cambridge, 1996, 269–296.
[18] P. Pollack, *Revisiting Gauss's analogue of the prime number theorem for polynomials over a finite field*, Finite Fields Appl. 16, (2010), 290–299.
[19] I. M. Sobol', *The distribution of points in a cube and the approximate evaluation of integrals*, USSR Comput. Math. Math. Phys. 7 (1967), no. 4, 86–112.
[20] S. Tezuka, *Polynomial arithmetic analogue of Halton sequences*, ACM Trans. Model. Comput. Simul. 3 (1993), 99–107.
[21] S. Tezuka, *Uniform Random Numbers: Theory and Practice*, Kluwer, Boston, 1995.
[22] S. Tezuka, *On the discrepancy of generalized Niederreiter sequences*, J. Complexity 29 (2013), 240–247.
[23] http://www.mathworks.com/help/stats/sobolset.html (Matlab function *sobolset*).
[24] http://cran.r-project.org/web/packages/randtoolbox/randtoolbox.pdf (R package *randtoolbox*).

Henri Faure
Aix-Marseille Université
CNRS, Centrale Marseille, I2M, UMR 7373
13453 Marseille, France
E-mail: henri.faure@univ-amu.fr

Christiane Lemieux
Department of Statistics
and Actuarial Science
University of Waterloo
200 University Avenue West
Waterloo, ON N2L 3G1, Canada
E-mail: clemieux@uwaterloo.ca

Abstract (will appear on the journal's web site only)

Sobol' sequences are a popular family of low-discrepancy sequences, in spite of requiring primitive polynomials instead of irreducible ones in later constructions by Niederreiter and Tezuka. We introduce a generalization of Sobol' sequences that removes this shortcoming and that we believe has the potential of becoming useful for practical applications. Indeed, these sequences preserve two important properties of the original construction proposed by Sobol': their generating matrices are non-singular upper triangular matrices, and they have an easy-to-implement column-by-column construction. We prove they form a subfamily of the wide family of generalized Niederreiter sequences, hence satisfying all known discrepancy bounds for this family. Further, their connections with Niederreiter sequences show these two families only have a small intersection (after reordering the rows of generating matrices of Niederreiter sequences in that intersection).